Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	10-154976	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 13:24
L2	1079	des with mask	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 13:28
L3	12	l2 with encrypt$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 13:28
L4	0	(RC5 or RC6) with mask	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 13:28
L5	1	(RC5 or RC6) same mask	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 13:28
L6	3046	des same mask	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 13:29
L7	67	l6 same (encrypt$3 or encipher$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 13:30
L8	29	des same ((extract or remove) near3 mask)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 13:31
L9	0	l8 same (encrypt$3 or encipher$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 13:31

L10	10495	((extract or remove) near3 mask)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 13:31
L11	4	l10 same (encrypt$3 or encipher$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 13:31

Published before August 1999
Terms used **removing mask encryption power analysis**

Found **27** of **99,277**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 27 Result page: **1** 2 next

Relevance scale

1 Security Mechanisms in High-Level Network Protocols
Victor L. Voydock, Stephen T. Kent
June 1983 **ACM Computing Surveys (CSUR)**, Volume 15 Issue 2
Full text available: pdf(3.23 MB) Additional Information: full citation, references, citings

2 Recursive hashing functions for n-grams
Jonathan D. Cohen
July 1997 **ACM Transactions on Information Systems (TOIS)**, Volume 15 Issue 3
Full text available: pdf(361.86 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Many indexing, retrieval, and comparison methods are based on counting or cataloguing n-grams in streams of symbols. The fastest method of implementing such operations is through the use of hash tables. Rapid hashing of consecutive n-grams is best done using a recursive hash function, in which the hash value of the current n-gram is drived from the hash value of its predecessor. This article generalizes recursive hash functions found in the ...

Keywords: n-grams, hashing, hashing functions, recursive hashing

3 Fast detection of communication patterns in distributed executions
Thomas Kunz, Michiel F. H. Seuren
November 1997 **Proceedings of the 1997 conference of the Centre for Advanced Studies on Collaborative research**
Full text available: pdf(4.21 MB) Additional Information: full citation, abstract, references, index terms

Understanding distributed applications is a tedious and difficult task. Visualizations based on process-time diagrams are often used to obtain a better understanding of the execution of the application. The visualization tool we use is Poet, an event tracer developed at the University of Waterloo. However, these diagrams are often very complex and do not provide the user with the desired overview of the application. In our experience, such tools display repeated occurrences of non-trivial commun ...

4 Illustrative risks to the public in the use of computer systems and related technology
Peter G. Neumann
January 1996 **ACM SIGSOFT Software Engineering Notes**, Volume 21 Issue 1
Full text available: Additional Information:

pdf(2.54 MB) full citation

5 Performance analysis of MD5

Joseph D. Touch

October 1995 **ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication**, Volume 25 Issue 4

Full text available: pdf(1.04 MB) Additional Information: full citation, abstract, references, citings, index terms

MD5 is an authentication algorithm proposed as the required implementation of the authentication option in IPv6. This paper presents an analysis of the speed at which MD5 can be implemented in software and hardware, and discusses whether its use interferes with high bandwidth networking. The analysis indicates that MD5 software currently runs at 85 Mbps on a 190 Mhz RISC architecture, a rate that cannot be improved more than 20-40%. Because MD5 processes the entire body of a packet, this data ra ...

6 Audience analysis in cyberspace: defining the invisible

Lisa Rosenberger

November 1998 **ACM SIGDOC Asterisk Journal of Computer Documentation**, Volume 22 Issue 4

Full text available: pdf(491.38 KB) Additional Information: full citation, index terms

7 Integrating security in a large distributed system

M. Satyanarayanan

August 1989 **ACM Transactions on Computer Systems (TOCS)**, Volume 7 Issue 3

Full text available: pdf(2.90 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Andrew is a distributed computing environment that is a synthesis of the personal computing and timesharing paradigms. When mature, it is expected to encompass over 5,000 workstations spanning the Carnegie Mellon University campus. This paper examines the security issues that arise in such an environment and describes the mechanisms that have been developed to address them. These mechanisms include the logical and physical separation of servers and clients, support for secure communication ...

8 Watermarking techniques for intellectual property protection

A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, G. Wolfe

May 1998 **Proceedings of the 35th annual conference on Design automation - Volume 00**

Full text available: pdf(243.93 KB) Additional Information: full citation, abstract, references, citings, index terms

Publisher Site

Digital system designs are the product of valuable effort and know-how. Their embodiments, from software and HDL program down to device-level netlist and mask data, represent carefully guarded intellectual property (IP). Hence, design methodologies based on IP reuse require new mechanisms to protect the rights of IP producers and owners. This paper establishes principles of watermarking-based IP protection, where a watermark is a mechanism for identificatio ...

Keywords: intellectual property test, system-on-chip test, testing embedded core

9 A structural view of the Cedar programming environment

Daniel C. Swinehart, Polle T. Zellweger, Richard J. Beach, Robert B. Hagmann

August 1986 **ACM Transactions on Programming Languages and Systems (TOPLAS)**, Volume 8 Issue 4

Full text available: pdf(6.32 MB) Additional Information: full citation, abstract, references, citings, index terms

This paper presents an overview of the Cedar programming environment, focusing on its overall structure—that is, the major components of Cedar and the way they are organized. Cedar supports the development of programs written in a single programming language, also called Cedar. Its primary purpose is to increase the productivity of programmers whose activities include experimental programming and the development of prototype software systems for a high-performance personal computer. T ...

10 Pen computing: a technology overview and a vision

André Meyer

July 1995 **ACM SIGCHI Bulletin**, Volume 27 Issue 3

Full text available: pdf(5.14 MB) Additional Information: full citation, abstract, citings, index terms

This work gives an overview of a new technology that is attracting growing interest in public as well as in the computer industry itself. The visible difference from other technologies is in the use of a pen or pencil as the primary means of interaction between a user and a machine, picking up the familiar pen and paper interface metaphor. From this follows a set of consequences that will be analyzed and put into context with other emerging technologies and visions.Starting with a short historic ...

11 Multicast security and its extension to a mobile environment

Li Gong, Nachum Shacham

March 1995 **Wireless Networks**, Volume 1 Issue 3

Full text available: pdf(1.22 MB) Additional Information: full citation, abstract, references, citings

Multicast is rapidly becoming an important mode of communication and a good platform for building group-oriented services. To be used for trusted communication, however, current multicast schemes must be supplemented by mechanisms for protecting traffic, controlling participation, and restricting access of unauthorized users to data exchanged by the participants. In this paper, we consider fundamental security issues in building a trusted multicast facility. We discuss techniques for group- ...

12 Distributed systems - programming and management: On remote procedure call

Patrícia Gomes Soares

November 1992 **Proceedings of the 1992 conference of the Centre for Advanced Studies on Collaborative research - Volume 2**

Full text available: pdf(4.52 MB) Additional Information: full citation, abstract, references, citings

The Remote Procedure Call (RPC) paradigm is reviewed. The concept is described, along with the backbone structure of the mechanisms that support it. An overview of works in supporting these mechanisms is discussed. Extensions to the paradigm that have been proposed to enlarge its suitability, are studied. The main contributions of this paper are a standard view and classification of RPC mechanisms according to different perspectives, and a snapshot of the paradigm in use today and of goals for t ...

13 Using the ASTRAL model checker to analyze mobile IP

Zhe Dang, Richard A. Kemmerer

May 1999 **Proceedings of the 21st international conference on Software engineering**

Full text available: pdf(1.16 MB) Additional Information: full citation, references, citings, index terms

Keywords: ASTRAL, Encryption protocols, formal methods, formal specification and verification, real-time systems, state machines, timing requirements

14 Secure audit logs to support computer forensics
Bruce Schneier, John Kelsey
May 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 2
Full text available: pdf(125.50 KB) Additional Information: full citation, abstract, references, citings, index terms, review

In many real-world applications, sensitive information must be kept it log files on an untrusted machine. In the event that an attacker captures this machine, we would like to guarantee that he will gain little or no information from the log files and to limit his ability to corrupt the log files. We describe a computationally cheap method for making all log entries generated prior to the logging machine's compromise impossible for the attacker to read, and also impossible to modify or dest ...

Keywords: audit logs, auditing, authenthication, computer forensics, hash chains, intrusion detection

15 Behavioral synthesis techniques for intellectual property protection
Inki Hong, Miodrag Potkonjak
June 1999 **Proceedings of the 36th ACM/IEEE conference on Design automation**
Full text available: pdf(157.64 KB) Additional Information: full citation, references, citings, index terms

16 Application access control at network level
Refik Molva, Erich Rütsche
November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security**
Full text available: pdf(956.82 KB) Additional Information: full citation, abstract, references, index terms

This paper describes an access control mechanism that enforces at the network level an access control decision that is taken at the application level. The mechanism is based on the pre-computation of encrypted counters called tickets. An access enforcement device verifies the existence of a valid ticket in each packet that is subject to access control and kills unauthorized packets. Tickets are not computed as a function of the user data. Due to the timing constraints of shared media LANs t ...

17 ASHs: Application-specific handlers for high-performance messaging
Deborah A. Wallach, Dawson R. Engler, M. Frans Kaashoek
August 1996 **ACM SIGCOMM Computer Communication Review , Conference proceedings on Applications, technologies, architectures, and protocols for computer communications**, Volume 26 Issue 4
Full text available: pdf(174.50 KB) Additional Information: full citation, abstract, references, citings, index terms

Application-specific safe message handlers (ASHs) are designed to provide applications with hardware-level network performance. ASHs are user-written code fragments that safely and efficiently execute in the kernel in response to message arrival. ASHs can direct message transfers (thereby eliminating copies) and send messages (thereby reducing send-response latency). In addition, the ASH system provides support for dynamic integrated layer processing (thereby eliminating duplicate message ...

18 New design concepts for an intelligent Internet
Geng-Sheng Kuo, Jing-Pei Lin
November 1998 **Communications of the ACM**, Volume 41 Issue 11
Full text available: pdf(153.32 KB) Additional Information: full citation, references, index terms

19 Death, taxes, and imperfect software: surviving the inevitable
Crispin Cowan, Calton Pu
January 1998 **Proceedings of the 1998 workshop on New security paradigms**
Full text available: pdf(1.09 MB) Additional Information: full citation, references, index terms

20 Cluster-based scalable network services
Armando Fox, Steven D. Gribble, Yatin Chawathe, Eric A. Brewer, Paul Gauthier
October 1997 **ACM SIGOPS Operating Systems Review , Proceedings of the sixteenth ACM symposium on Operating systems principles**, Volume 31 Issue 5
Full text available: pdf(2.42 MB) Additional Information: full citation, references, citings, index terms

Results 1 - 20 of 27 Result page: **1** 2 next

Published before August 1999
Terms used **removing mask encryption power analysis**

Found **27** of **99,277**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 21 - 27 of 27 Result page: previous 1 **2**

Relevance scale

21 Fast compilation for pipelined reconfigurable fabrics
Mihai Budiu, Seth Copen Goldstein
February 1999 **Proceedings of the 1999 ACM/SIGDA seventh international symposium on Field programmable gate arrays**
Full text available: pdf(2.03 MB) Additional Information: full citation, references, citings, index terms

22 Before the Altair: the history of personal computing
Larry Press
September 1993 **Communications of the ACM**, Volume 36 Issue 9
Full text available: pdf(2.51 MB) Additional Information: full citation, references, citings, index terms

23 PipeRench: a co/processor for streaming multimedia acceleration
Seth Copen Goldstein, Herman Schmit, Matthew Moe, Mihai Budiu, Srihari Cadambi, R. Reed Taylor, Ronald Laufer
May 1999 **ACM SIGARCH Computer Architecture News , Proceedings of the 26th annual international symposium on Computer architecture**, Volume 27 Issue 2
Full text available: pdf(202.69 KB) Publisher Site Additional Information: full citation, abstract, references, citings, index terms

Future computing workloads will emphasize an architecture's ability to perform relatively simple calculations on massive quantities of mixed-width data. This paper describes a novel reconfigurable fabric architecture, PipeRench, optimized to accelerate these types of computations. PipeRench enables fast, robust compilers, supports forward compatibility, and virtualizes configurations, thus removing the fixed size constraint present in other fabrics. For the first time we explore how the bit-widt ...

24 Comparing information without leaking it
Ronald Fagin, Moni Naor, Peter Winkler
May 1996 **Communications of the ACM**, Volume 39 Issue 5
Full text available: pdf(344.25 KB) Additional Information: full citation, references, citings, index terms

25 The Legion vision of a worldwide virtual computer
Andrew S. Grimshaw, Wm. A. Wulf, CORPORATE The Legion Team

January 1997 **Communications of the ACM**, Volume 40 Issue 1
Full text available: pdf(1.00 MB) Additional Information: full citation, references, citings, index terms, review

26 On the influence of scale in a distributed system
M. Satyanarayanan
April 1988 **Proceedings of the 10th international conference on Software engineering**
Full text available: pdf(1.10 MB) Additional Information: full citation, abstract, references, citings, index terms

Scale should be recognized as a primary factor influencing the architecture and implementation of distributed systems. This paper uses Andrew, a distributed environment at Carnegie Mellon University, to validate this proposition. The design of Andrew is dominated by considerations of performance, operability and security. Caching of information and placing trust in as few machines as possible emerge as two general principles that enhance scalability. The separation of concerns made possible ...

27 Position papers: Legion: flexible support for wide-area computing
Andrew S. Grimshaw, William A. Wulf
September 1996 **Proceedings of the 7th workshop on ACM SIGOPS European workshop: Systems support for worldwide applications**
Full text available: pdf(921.19 KB) Additional Information: full citation, references

Your search matched **1** of **1140634** documents.
A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance** in **Descending** order.

Refine This Search:
You may refine your search by editing the current search expression or entering a new one in the text box.

removing mask Search

☐ Check to search within this result set

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

---

1 **Two pixel-preselection methods for median-type filtering**
Garcia-Cabrera, L.; Luque-Escamilla, P.L.; Martinez-Aroza, J.; Robles-Perez, A.M.; Roman-Roldan, R.;
Vision, Image and Signal Processing, IEE Proceedings- , Volume: 145 , Issue: 1 , Feb. 1998
Pages:30 - 40

[Abstract] [PDF Full-Text (3248 KB)] **IEE JNL**

Google Web Images Groups News Froogle Local[New!] more »
"removing mask " encryption Search Advanced Search Preferences

Web

Results **1** - **5** of about **12** for **"removing mask " encryption**. (**0.55** seconds)

5321852 Circuit and method for converting a radio frequency signal ...
... system apparatus and methods 380/20 5321749 **Encryption** device 380 ... crystal device including masking areas between electrodes, rubbing, **removing mask**, and rubbing ...
ftp.std.com/obi/Patents/Titles/940614 - 101k - Supplemental Result - Cached - Similar pages

Zeropaid Forums - Way to defeat the traceable hash of an MP3?
... Or....you could just get one of those IDE inline **encryption** doooohickies then pull the damn thing if/when you get a notice from the RIAA...lol. Reply With Quote ...
www.zeropaid.com/bbs/showthread.php?p=161078 - 69k - Supplemental Result - Cached - Similar pages

United States Patent Application: 0020130315
... In such an application, a quantum computer could render obsolete all existing **encryption** schemes that use the "public key" method. ...
appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO2& Sect2=HITOFF&p=2&u=%2Fnetahtml%2FPTO%2Fsearch-... - 65k - Supplemental Result - Cached - Similar pages

[PDF] IP Routing Protocols Commands
File Format: PDF/Adobe Acrobat - View as HTML
... The password is encrypted in the configuration file if the service password-**encryption** command is enabled. There is no default value. ...
www.prz.tu-berlin.de/docs/misc/ ciscodoc/data/doc/software/11_0/accr/ariprout.pdf - Supplemental Result - Similar pages

[PDF] Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and ...
File Format: PDF/Adobe Acrobat - View as HTML
... Module SC/SR: • AAA Security Services • Security Server Protocols • Traffic Filtering and Firewalls • IP Security and **Encryption** • Passwords and ...
netadm.pasteur.fr/cisco/IOS_12.2/1rfbook1.pdf - Supplemental Result - Similar pages

In order to show you the most relevant results, we have omitted some entries very similar to the 5 already displayed.
If you like, you can repeat the search with the omitted results included.

"removing mask " encryption Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google